PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4665 di Giovedì 26 marzo 2020

Va bene lo smart working, ma fate attenzione!

Nell'attuale situazione molte aziende hanno accettato l'invito del Governo e organizzato con i propri dipendenti, il lavoro da casa in telelavoro. La soluzione è attraente, ma occorre fare molta attenzione all'aumento dei rischi informatici.

La crescente diffusione dello smart working, del tutto comprensibile per determinate attività ed in circostanze critiche, come le presenti, può comportare un aumento di rischi, sui quali forse i dipendenti non sono stati sufficientemente sensibilizzati.

Questa è la ragione per la quale il servizio segreto degli Stati Uniti ha lanciato un messaggio di sensibilizzazione, indirizzato a tutti coloro che si trovano nella condizione sopra illustrata, illustrando rischi specifici, che vengono grandemente aumentati, in conseguenza dell'aumento delle persone che operano in smart working.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0499] ?#>

Sono state già registrate numerosi frodi informatiche, che utilizzano i sistemi di posta elettronica.

Ad esempio, alcune frodi utilizzano tattiche di ingegneria sociale per chiedere donazioni in favore di organizzazioni, impegnate sul fronte della gestione del contagio di COVID 19, invitando i destinatari dei messaggi ad effettuare donazioni, fornendo anche dati personali per inviare un messaggio di ringraziamento.

Il truffatore, con questo tipo di attacco, non solo acquisisce la donazione, ma acquisisce anche dati personali, che possono essere utilizzati per portare a termine altre frodi.

Un altro tipo di frode informatica, che in Italia potrebbe essere particolarmente fruttuoso, riguarda l'offerta a prezzo allettante di presidi sanitari, in particolare mascherine e disinfettanti per le mani: il destinatario di questo messaggio, come purtroppo spesso avviene, invia il denaro e non riceve nulla.

Poiché, insieme all'invio del denaro, egli deve fornire il proprio indirizzo, la frode può essere sviluppata ulteriormente, effettuando a domicilio una consegna di un pacco vuoto.

Se il destinatario reclama, il truffatore dichiara che probabilmente si è trattato di un disguido, oppure di un intervento fraudolento da parte del corriere; il truffatore dichiara di aver avviato una pratica per ricostruire l'accaduto e guadagna giorni preziosi, per cancellare le tracce del suo operato.

Alla luce di questi eventi, ritengo opportuno che il datore di lavoro sensibilizzi tutti i dipendenti nel prestare massima attenzione alla ricezione di messaggi di posta elettronica, di origine anche solo sospetta, segnalando l'accaduto al responsabile informatico.

Quest'ultimo si potrà rendere meglio conto della situazione, se ad esempio tutti i dipendenti di una stessa azienda vengono raggiunti da una simile messaggio di posta elettronica.

In questo caso, è probabile che il malvivente sia riuscita a violare l'elenco degli indirizzi di posta elettronica dei dipendenti ed abbia avviato una una specifica attività fraudolenta.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it